

1 John M. Desmarais (SBN 320875)
DESMARAIS LLP
2 101 California Street
San Francisco, CA 94111
3 (415) 573-1900

4 Tamir Packin (SBN 317249)
Carson Olsheski (*pro hac vice* pending)
5 DESMARAIS LLP
230 Park Avenue
6 New York, NY 10169
212-351-3400

7 *Attorneys for Plaintiffs*

8
9
10 **UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

11 **CISCO SYSTEMS, INC., a California
12 Corporation, CISCO TECHNOLOGY, INC., a
California Corporation**

13 **Plaintiffs,**

14 **v.**

15 **PLANTRONICS, INC., a Delaware
16 Corporation, WILSON CHUNG, JAMES HE,
JEDD WILLIAMS, AND THOMAS
17 PUORRO individuals**

18 **Defendants.**

Case No.: 3:19-cv-07562-PJH

JURY TRIAL DEMANDED

19 **FIRST AMENDED COMPLAINT FOR TRADE SECRET MISAPPROPRIATION**

20
21 Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (collectively “Cisco”), for their
22 Complaint against Defendants Plantronics, Inc. (“Poly”), Wilson Chung (“Dr. Chung”), James He
23 (“Mr. He”), Jedd Williams (“Mr. Williams”), and Thomas Puorro (“Mr. Puorro”) hereby allege as
24 follows:

25 **Introduction**

26 1. This is an action for trade secret misappropriation by Poly and the named parties, all of
27 whom are former Cisco employees and are current or former Poly employees. Mr. Puorro, a former
28 Cisco executive and the current Executive Vice President, General Manager, Products at Poly

1 responsible for Poly's audio and video collaboration solutions, orchestrated a scheme on behalf of
2 Poly to induce Cisco employees to reveal trade secrets to him and others at Poly in an effort to unfairly
3 compete against Cisco and to "inflict pain" upon Cisco. This scheme was endorsed by Poly's most
4 senior executives, who had knowledge of, and acquiesced to, Mr. Puorro's tactics. Even after Cisco
5 brought the egregious misconduct to the attention of Poly, Poly refused to disavow the theft of Cisco's
6 trade secrets and continues to shield its employees and executives. Cisco brings this suit against Poly
7 because of Poly's continued endorsement of the scheme and its failure to take corrective action, even
8 when presented with overwhelming evidence of misconduct.

9 2. Cisco has invested significant resources to design, build, and sell its robust
10 collaboration platform, which includes unified communications and video conferencing software and
11 collaboration endpoints. Cisco's endpoint hardware includes video endpoints, telepresence units, all-
12 in-one video collaboration systems, integrated collaboration room systems, VoIP and video phones,
13 microphones, cameras, speakers, and headsets. The collaboration field is highly competitive and
14 characterized by rapid innovation. Cisco's engineers rely upon tangible and intangible financial,
15 business, scientific, technical, economic, and engineering information, such as source code,
16 schematics, design details and specifications, user feedback, design documentation, and feature
17 documentation relating to Cisco's existing and future products, as well as Cisco business information
18 such as operations, marketing, and resource strategies and plans, supplier information, cost and pricing
19 information, and payment information to develop Cisco's products. Cisco takes reasonable measures
20 to keep this information secret, and this information derives independent economic value from not
21 being generally known to, and not being readily ascertainable through proper means by, others who
22 can obtain economic value from the disclosure or use of the information.

23 3. Cisco also has made substantial and significant investments in developing its routes to
24 market for its collaboration products and services, through extensive engagement of partner, customer,
25 and industry connections by its global sales force. Cisco's global sales force relies upon tangible and
26 intangible financial, business, and economic information, such as non-public financial reporting,
27 customer lists, pricing models, forecasting, sales, resourcing, and competitive strategies and plans, and
28 product refresh strategies to develop Cisco's go-to-market and business development plans and to

1 market and sell Cisco products. Cisco takes reasonable measures to keep this information secret, and
2 this information derives independent economic value from not being generally known to, and not being
3 readily ascertainable through proper means by, others who can obtain economic value from the
4 disclosure or use of the information.

5 4. Cisco has uncovered evidence that Dr. Chung and Mr. He, two former high-level
6 engineers in Cisco's Unified Communications Technology Group, downloaded thousands of
7 documents containing Cisco's highly confidential and proprietary business information ("Cisco
8 Confidential Materials") relating to the design, manufacture, pricing, and market opportunities for
9 both current and unreleased products. Dr. Chung undertook efforts over a period of weeks preceding
10 his departure, and after he had accepted employment with Poly and while he was, unbeknownst to
11 Cisco, simultaneously employed by both Cisco and Poly, to exfiltrate Cisco Confidential Materials to
12 removable hard drives, personal email, cloud storage, and to Poly's internal intranet, and then used
13 Cisco Confidential Materials while at Poly. When confronted with evidence of his misappropriation,
14 Dr. Chung destroyed evidence to conceal his actions.

15 5. Mr. He joined Poly after being recruited by Dr. Chung. Prior to his departure, and after
16 accepting his employment offer from Poly, Mr. He copied thousands of files containing Cisco
17 Confidential Materials to an external hard drive. These documents also related to the design,
18 manufacture, pricing, and market opportunities for both current and unreleased products. Cisco has
19 recovered Mr. He's hard drive, and learned that Mr. He accessed a number of these documents while
20 at Poly, and, when the misappropriation was uncovered, deleted the files to avoid detection.

21 6. Cisco also has uncovered evidence that Mr. Williams misappropriated Cisco
22 Confidential Materials relating to Cisco's financial information and sales, business development,
23 resourcing and competitive strategies and plans, including Cisco's market data and strategies, partner
24 margins, potential organizational restructurings, information concerning Cisco's emerging
25 technologies, competitive focus, sales opportunities and customer lists, product pipelines, and future
26 plans for current products. On information and belief, Mr. Williams disclosed Cisco Confidential
27 Materials to senior executives at Poly during the recruiting and interview process and exfiltrated these
28 materials from Cisco, including by storing an unauthorized backup of his Cisco laptop on a home

1 server and maintaining Cisco Confidential Materials on that server after leaving Cisco and starting
2 work at Poly. Cisco also has uncovered evidence suggesting that Mr. Williams was offered
3 employment at Poly after proposing and disclosing to Poly Cisco Confidential Materials, including a
4 non-public go-to-market strategy he dubbed “Project x,” which had been developed and refined at
5 Cisco and was therefore Cisco’s proprietary information, and which he disclosed while employed by
6 Cisco to both Mr. Puorro and at least two other very high ranking Poly executives.

7 7. Cisco has also uncovered evidence that Mr. Puorro, a former Cisco executive, and
8 Executive Vice President at Poly, induced Mr. Williams to reveal Cisco’s trade secrets to him and to
9 other senior executives at Poly. As a former Cisco executive, Mr. Puorro was, or should have been,
10 familiar with Cisco’s confidentiality policies, and knew, or should have known, that the information
11 he requested from Mr. Williams contained Cisco trade secrets and that his request for and receipt of
12 such information interfered with Mr. Williams’ obligations to Cisco.

13 8. In sum, Dr. Chung, Mr. He, Mr. Williams, and Mr. Puorro engaged in a scheme that
14 on information and belief was endorsed by senior Poly executives and was designed to give Poly
15 access to Cisco’s trade secrets and allow Poly to unfairly compete with Cisco.

16 9. Defendants’ conduct threatens to cause Cisco irreparable harm, potentially depriving
17 Cisco of the opportunity to obtain a first-mover advantage in product development and go-to-market
18 strategies, and depriving Cisco of business opportunities. There is also the threat that Cisco
19 Confidential Materials will be further disclosed by Defendants, which will damage Cisco’s trade secret
20 technology and business processes.

21 **The Parties**

22 10. Plaintiff Cisco Systems, Inc., is a company duly organized and existing under the laws
23 of California, having its principal place of business at 170 West Tasman Drive, San Jose, California
24 95134.

25 11. Plaintiff Cisco Technology, Inc. is a wholly owned subsidiary of Cisco Systems, Inc.,
26 and is a company duly organized and existing under the laws of California, having its principal place
27 of business at 170 West Tasman Drive, San Jose, California 95134.

12. Defendant Poly is a Delaware corporation, with its principal place of business at 345 Encinal Street, Santa Cruz, California 95060. Poly may be served with process by serving its registered agent, CT Corporation System, 818 W. Seventh Street, Ste. 930, Los Angeles, CA 90017. Poly is in the IP telephony, headset, video, and collaboration space, and is a competitor to Cisco.

13. Dr. Chung is an individual residing in this jurisdiction.

14. Mr. He is an individual residing in this jurisdiction.

15. Mr. Williams is an individual residing outside this jurisdiction.

16. Mr. Puorro is an individual residing outside this jurisdiction.

Nature Of The Action

17. This is a civil action for violation of the Defend Trade Secrets Act (“DTSA”) under 18 U.S.C. § 1836 *et seq.*, violation of Cal. Civ. Code § 3426 *et seq.*, and Intentional Interference with a Contractual Relationship.

Jurisdiction And Venue

18. This Court has subject matter jurisdiction over Cisco’s claims for violation of the Defend Trade Secrets Act (“DTSA”) pursuant to 28 U.S.C. §§ 1331 because they present a Federal Question.

19. This Court has supplemental subject matter jurisdiction of the pendent state law claims pursuant to 28 U.S.C. § 1367 because they are so related to the DTSA claims that they form part of the same case or controversy.

20. This Court has personal jurisdiction over Poly because its principal place of business is in this district.

21. This Court has personal jurisdiction over Dr. Chung because he resides in this district.

22. This Court has personal jurisdiction over Mr. He because he resides in this district.

23. This Court has personal jurisdiction over Mr. Williams at least because he has purposefully directed his activities to this forum by committing intentional acts within California causing harm to Cisco (a California corporation). Mr. Williams also purposefully directed his activities to this forum and residents thereof, by disclosing Cisco’s trade secrets to Poly and its officers, including those at Poly’s California headquarters, so that Mr. Williams could obtain a job at Poly. Mr.

Williams also purposefully directed his activities to this forum through his repeated travels to California to interview with Poly, and by beginning employment with Poly in California, and by agreeing that his confidentiality obligations to Cisco shall be interpreted and enforced in accordance with the laws of the State of California. Mr. Williams also carried on a continuous course of communications with Poly's executives in California, including communications giving rise to the claims at issue in this case. Moreover, the claims arise out of Mr. Williams' activities within the forum. For example, as outlined in the detailed factual allegations below, Mr. Williams revealed Cisco's trade secrets to Poly while in California, including on or around April 1, 2019, April 30, 2019, and June 28, 2019. Mr. Williams also created the contacts giving rise to the claims at issue in this case with the forum himself, at least through his frequent and voluntary travels to Poly's headquarters in California while seeking employment. Furthermore, Mr. Williams certified to Poly on October 12 that he did not then possess any Cisco Confidential Materials or property. Both Mr. Williams and Poly knew that Mr. Williams' certification was false since, among other things, they knew Mr. Williams was still employed at Cisco and Mr. Williams had access to Cisco Confidential Materials. Indeed, the falsity of Mr. Williams' certification is evidenced by, among other things, the fact that he uploaded Cisco Confidential Materials to a Cisco cloud storage site while he was in California after executing the certification, he personally returned his Cisco laptop to Cisco in California after executing the certification, and never returned the backup of his Cisco laptop that he created. The false certification instigated from Poly's California office—which Poly either knew, or should have known, was meaningless—evidences that neither Mr. Williams nor Poly undertook reasonable protection of Cisco Confidential Materials.

24. This Court has personal jurisdiction over Mr. Puorro at least because Mr. Puorro purposefully directed his activities to this forum, by misappropriating Cisco's trade secrets for the benefit of Poly, a corporation with its principal place of business in California. In particular, Mr. Puorro carried on a continuous course of direct communications with Poly's executives in California, including the communications giving rise to the claims at issue in this case, such as his advocacy for Mr. Williams' hiring to Poly's senior executives in California. As outlined in the detailed factual allegations below, Mr. Puorro was also the guiding spirit behind Poly's wrongful conduct at issue in

1 this case. Moreover, the claim arises out of Mr. Puorro's activities within the forum. For example, as
 2 outlined in the detailed factual allegations below, Messrs. Puorro and Williams were together in
 3 California from April 2-5, 2019, and met in person to discuss Mr. Williams' potential employment at
 4 Poly, and Cisco's collaboration product portfolio. These April meetings occurred after Mr. Williams
 5 began relaying confidential details of Cisco's business to Mr. Puorro in exchange for Mr. Puorro
 6 promoting Mr. Williams' employment candidacy. On information and belief, this course of conduct
 7 continued during the April meetings between Messrs. Puorro and Williams in California. Moreover,
 8 Mr. Puorro traveled to Santa Cruz during the week of July 1st. In that week, Mr. Puorro solicited
 9 confidential information about Cisco from Mr. Williams.

10 25. Venue is proper within this District under 28 U.S.C. § 1391(b) because a substantial
 11 part of the events or omissions giving rise to these claims occurred within this District.

12 **FACTUAL ALLEGATIONS**

13 **A. Dr. Chung**

14 26. Dr. Chung was employed at Cisco as Principal Engineer in Cisco's Unified
 15 Communications Technology Group ("UCTG"). Dr. Chung was involved in developing Cisco's
 16 collaboration products, including IP telephony solutions and audio headsets. Incumbent with this role
 17 was access to some of Cisco's most confidential trade secrets used within the UCTG, including design
 18 specifications, schematics, source code, product market analyses, and vendor contract details. On
 19 information and belief, after joining Poly, Mr. Puorro recruited Dr. Chung, and as a result of these
 20 efforts, Dr. Chung left Cisco in February 2019 to join Poly. Before doing so, Dr. Chung willfully and
 21 maliciously misappropriated Cisco Confidential Materials to use for his own benefit, and for the
 22 benefit of Poly, to the detriment of Cisco. Almost immediately after starting at Poly, Dr. Chung carried
 23 out Poly and Mr. Puorro's efforts to entice Cisco's collaboration engineers to join Poly by recruiting
 24 his former colleague, James He.

25 27. Dr. Chung began working for Cisco as a Technical Leader in March 2007.

26 28. On May 7, 2012, Dr. Chung became Principal Engineer of Cisco's UCTG.

27 29. Dr. Chung claims that his personal and Cisco laptops were stolen around Thanksgiving
 28 2018.

1 30. Subsequent to the alleged theft, Dr. Chung used a Lenovo ThinkPad X1 with serial
2 number PF0Z3DLE (“Lenovo laptop”) issued by Cisco as his primary work computer.

3 31. On November 14, 2018, Cisco also leased a MacBook Pro from IBM Global Finance
4 which was assigned to Dr. Chung to use as a secondary work computer. Dr. Chung’s department
5 incurred the cost for this MacBook Pro. This MacBook Pro (serial number C02W186W186HV2M)
6 (“MacBook”) was shipped to Cisco and later delivered to Dr. Chung.

7 32. Dr. Chung does not own, and has never owned, the MacBook.

8 33. Dr. Chung is not the lessee, and has never been the lessee, of the MacBook.

9 34. Cisco did not authorize Dr. Chung’s retention of the MacBook when his employment
10 with Cisco ended.

11 35. Dr. Chung has no right to possess the MacBook after his employment with Cisco
12 terminated, and also had no right to possess the MacBook when he began to work at Poly.

13 36. On February 3, 2019, Dr. Chung downloaded over 3,000 files from Cisco’s internal
14 document repositories. These documents are Cisco Confidential Materials and relate to, among other
15 things, Cisco’s contributions to 5G technology (such as its market opportunities), and design
16 specifications of a pre-release video conferencing display prototype.

17 37. On February 3, 2019, Dr. Chung connected a Seagate Expansion Drive with serial
18 number NAA77962 (“First Seagate Drive”) to his Lenovo Laptop.

19 38. Dr. Chung has not made the First Seagate Drive available for inspection by either Cisco
20 or, according to Poly’s General Counsel, to Poly.

21 39. On February 3, 2019, Dr. Chung connected a Samsung Flash Drive with serial number
22 374718110032913 (“Samsung Drive”) to his Lenovo laptop five times.

23 40. Dr. Chung copied Cisco Confidential Materials to the Samsung Drive.

24 41. On February 3, 2019, Dr. Chung uploaded files from the MacBook to his personal
25 iCloud account, including Cisco’s source code for debugging a user interface.

26 42. On February 6, 2019, Dr. Chung copied 129 files containing Cisco Confidential
27 Materials that relate to vendor product roadmaps and a pre-release video conferencing display
28 prototype to a Seagate Expansion SCSI Disk Device with serial number 26977AAN (“Second Seagate

1 Drive”). The pre-release video conferencing display prototype documents included user experience
2 design documentation, user interview feedback, artwork prototypes, and schematics.

3 43. On February 6, 2019, Dr. Chung connected the Samsung Drive to the Lenovo laptop
4 four times.

5 44. On February 6, 2019, Dr. Chung connected a Sandisk UltraFit storage drive with serial
6 number 4C50001291121118332 (“Sandisk Drive”) to his Lenovo laptop two times.

7 45. On information and belief, on February 6, 2019, Dr. Chung uploaded a folder entitled
8 “Toyshop” from his Lenovo laptop to cloud storage. This folder included Cisco Confidential Materials
9 such as design details and specifications relating to Cisco’s collaboration endpoints, including Cisco’s
10 sound bar products.

11 46. Dr. Chung’s misappropriation of Cisco Confidential Materials was organized,
12 premeditated, and intentional.

13 47. On February 6, 2019, Dr. Chung created various folders on the Samsung Drive named
14 after an internal Cisco project codename.

15 48. On February 6, 7, and 8, 2019, Dr. Chung created various folders on the Second Seagate
16 Drive named after numerous additional Cisco project codenames.

17 49. On February 7, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
18 laptop.

19 50. On February 8, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
20 laptop twice.

21 51. On information and belief, on February 8, 2019, Dr. Chung uploaded Cisco
22 Confidential Materials to cloud storage, including a presentation detailing go-to-market strategy,
23 design details, cost modeling, and pricing information for a pre-release video conferencing display
24 product.

25 52. On February 9, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
26 laptop twice.

27 53. On February 10, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
28 laptop.

1 54. On February 11, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
2 laptop twice.

3 55. On February 12, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
4 laptop five times.

5 56. On February 13, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
6 laptop twice.

7 57. On February 13, 2019, the MacBook was physically connected to Cisco's corporate
8 network.

9 58. On February 13, 2019, Dr. Chung informed his manager that he was leaving Cisco.

10 59. During that February 13, 2019 conversation between Dr. Chung and his manager, Dr.
11 Chung told his manager that he was not sure where he would be working, but that he was considering
12 joining Apple.

13 60. On February 14, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
14 laptop four times.

15 61. Dr. Chung told Poly that his last day at Cisco was February 22, 2019.

16 62. Dr. Chung's last day at Cisco was, in fact, February 28, 2019.

17 63. Dr. Chung's exfiltration of Cisco Confidential Materials was outside the scope of his
18 employment at Cisco.

19 64. On February 24, 2019, Dr. Chung forwarded an email and attachment entitled "Cisco
20 UCaaS Market Position" from his Cisco email account to his personal Gmail account. The attached
21 document, clearly marked "Internal only" and "Cisco Confidential," related to Cisco's prospective
22 market positioning in the collaboration space.

23 65. On February 25, 2019, Dr. Chung downloaded more than 100 recordings of Webex
24 presentations to his Lenovo laptop. On information and belief, these recordings related to the design,
25 manufacture, pricing, and market opportunities for Cisco's Unified Communications product
26 portfolio.

27 66. On February 25, 2019, Dr. Chung connected the Second Seagate Drive to his Lenovo
28 laptop six times.

1 67. On February 25, 2019, Dr. Chung created a folder entitled “Webex_Recordings” on the
2 Second Seagate Drive.

3 68. From February 26, 2019 through February 28, 2019, Dr. Chung was an employee of
4 both Cisco and Poly.

5 69. On February 26, 2019, Dr. Chung began work at Poly.

6 70. On February 26, 2019, Dr. Chung logged into the MacBook.

7 71. On February 26, 2019, Dr. Chung emailed vendor representatives from his Cisco email
8 account to inform them that his last day at Cisco would be February 28, 2019.

9 72. On February 26, 2019, Dr. Chung forwarded an email from his Cisco email account to
10 his personal Gmail account. This email thread included “minutes” from a Cisco meeting.

11 73. On February 26, 2019, Dr. Chung logged into Poly’s “Sharepoint” site from the Lenovo
12 laptop. Dr. Chung uploaded to Poly’s Sharepoint, among other things, a spreadsheet entitled
13 Endpoints and Accessories (“EA Document”).

14 74. The EA Document contains Cisco Confidential Materials, including component
15 specifications and competitive differentiators for Cisco’s current and not yet released hardware
16 products.

17 75. On February 27, 2019, Dr. Chung forwarded an email from his Cisco email account to
18 his personal Gmail account with details about a vendor contract, which also included a payment terms.

19 76. On February 27, 2019, Dr. Chung accessed his Google drive from the Lenovo laptop.

20 77. On February 27, 2019, Dr. Chung went to Cisco’s office and returned his badge and
21 the Lenovo laptop to Cisco. Dr. Chung arrived at approximately 3:00pm, had coffee with a Cisco
22 colleague, and posed for a group photo with members of Cisco’s UCTG. Dr. Chung did not turn in
23 the MacBook, First Seagate Drive, Second Seagate Drive, SanDisk Drive, or Samsung Drive.

24 78. On February 28, 2019, Dr. Chung forwarded an email from his Cisco email account to
25 his personal Gmail account with details about sensor requirements for Cisco products.

26 79. On March 8, 2019, Dr. Chung emailed the EA Document from his personal Gmail
27 account to his Poly email account.

28

1 80. On March 8, 2019, Dr. Chung emailed a file marked as Cisco Confidential and entitled
2 “Webex Workplace Vision and Strategy – Compete” (“Webex Vision Document”) from his personal
3 Gmail account to his Poly email account.

4 81. By March 9, 2019, Dr. Chung began recruiting James He to join Poly.

5 82. As of March 28, 2019, the MacBook had not been returned to Cisco. Cisco contacted
6 Dr. Chung to secure return of the MacBook.

7 83. On March 29, 2019, Cisco contacted Dr. Chung and requested return of the MacBook.
8 Dr. Chung insisted that he owned the MacBook and asked Cisco to check with Cisco’s IT department.

9 84. On April 9, 2019, after checking with Cisco’s IT department, Cisco notified Dr. Chung
10 that the MacBook was Cisco property and must be returned. Dr. Chung subsequently confirmed that
11 he possessed the MacBook. Cisco followed up with Dr. Chung on April 10, April 11, April 14, April
12 15, and April 18, but Dr. Chung refused to return the MacBook.

13 85. Dr. Chung accessed Cisco Confidential Materials while employed at Poly, including at
14 least the EA Document, Webex Vision Document, and a Cisco collaboration roadmap document.

15 86. After being notified of Cisco’s concerns that Dr. Chung had misappropriated Cisco’s
16 trade secrets, on September 26, 2019, Poly informed Cisco that it had found five documents on Dr.
17 Chung’s devices that he used at Poly, including the EA Document that Dr. Chung had previously
18 uploaded to Poly’s Sharepoint.

19 87. Dr. Chung downloaded the EA Document from Poly’s Sharepoint to his new work
20 computer issued by Poly.

21 88. On information and belief, Dr. Chung accessed this file, and other documents
22 containing Cisco trade secret information, for his own benefit, and for the benefit of Poly, to Cisco’s
23 detriment.

24 89. On September 19, 2019, counsel for Cisco wrote Dr. Chung a letter putting Dr. Chung
25 on notice to preserve all documents and things related to the potential misappropriation of Cisco
26 Confidential Materials.

1 90. After receiving this preservation notice, Dr. Chung took steps to conceal his
2 misappropriation, including destroying evidence of his unlawful conduct. For example, after receiving
3 the preservation notice, Dr. Chung:

- 4 a. deleted iCloud backups;
- 5 b. deleted Cisco Confidential Materials from the MacBook;
- 6 c. deleted Cisco Confidential Materials from the Sandisk Drive;
- 7 d. deleted Cisco Confidential Materials from the Samsung Drive; and
- 8 e. propounded a demonstrably false explanation for failing to return the Second Seagate
9 Drive to Cisco.

10 91. After receiving this preservation notice, and before delivering the MacBook, Sandisk
11 Drive, his personal iPad, and Samsung Drive to his attorney to eventually return to Cisco, Dr. Chung
12 performed internet searches such as “how to permanently delete icloud backup,” and “how to see what
13 is [sic] the thumb drive without detection.”

14 92. Dr. Chung understood that his employment by Cisco created a relationship of
15 confidence and trust with respect to confidential and proprietary information, including Cisco
16 Confidential Materials. In order to protect Cisco Confidential Materials from use by a competitor, Dr.
17 Chung’s Proprietary Information and Inventions Agreement (“Chung PIIA”) prohibited Dr. Chung
18 during his employment with Cisco from becoming an employee of any other firm engaged in a
19 business in any way competitive with Cisco or involved in the design, development, marketing, sale,
20 or distribution of any networking or software products without first informing Cisco and obtaining its
21 consent.

22 93. By the terms of the Chung PIIA, Dr. Chung agreed that he would “not remove any
23 [Cisco] Documents and Materials from the business premises of [Cisco] or deliver any [Cisco]
24 Documents and Materials to any person or entity outside of [Cisco], except as [] required to do in
25 connection with performing the duties of [his] employment.” Dr. Chung also agreed that “immediately
26 upon the termination of [his] employment,” he would “return all [Cisco] Documents and Materials,
27 apparatus, equipment and other physical property, or any reproductions of such property”
28

1 94. Throughout its investigation into Dr. Chung's unlawful conduct, Cisco kept Poly
2 informed of the results of its ongoing investigation so that Poly could take necessary actions to remedy
3 the violations. With full knowledge of Dr. Chung's illegal activities, Poly inexplicably brought Dr.
4 Chung back to work on November 14, 2019, leaving Cisco no choice but to file this action to protect
5 its trade secrets. Indeed, as far back as September 9, 2019, Cisco first apprised Poly's General Counsel
6 of the results of Cisco's initial investigation into Dr. Chung's unlawful conduct. *See* Exhibit A. Cisco
7 followed up with Poly's General Counsel on September 19, 2019 to request a status of Poly's review
8 of the matter and further information regarding Dr. Chung's activities and employment at Poly. *See*
9 Exhibit B.

10 95. On or about September 27, 2019, Poly's General Counsel represented to Cisco that (a)
11 Poly had conducted an investigation into Dr. Chung's conduct, (b) Poly found that Dr. Chung had
12 indeed brought Cisco Confidential Materials with him to Poly, and (c) Dr. Chung told Poly that he did
13 not possess any Cisco equipment (even though he still had the MacBook Pro in his possession) and
14 proffered a demonstrably false explanation regarding his download activities on the Second Seagate
15 Drive and the whereabouts of the Second Seagate Drive. *See* Exhibit C. Cisco thereafter continued
16 its investigation into Dr. Chung's activities and his purported story to Poly. On October 9, 2019, Cisco
17 provided Poly with further details of Dr. Chung's illegal conduct, including that Dr. Chung was still
18 employed by Cisco when he accessed Cisco's systems and sent himself Cisco Confidential Materials
19 *while unbeknownst to Cisco* he also was employed at Poly, and requested that Poly take immediate
20 action to protect Cisco's intellectual property exfiltrated by Dr. Chung. *See* Exhibit D.

21 96. On October 10, 2019, Poly's General Counsel confirmed that Poly had placed Dr.
22 Chung on administrative leave. A subsequent forensic investigation by a neutral third-party of Dr.
23 Chung's devices and cloud accounts revealed that Dr. Chung accessed additional Cisco Confidential
24 Materials while employed at Poly, that he emailed Cisco Confidential Materials from his personal
25 email address to his Poly email address, and that apparent data wiping procedures were performed on
26 his devices. On the evening of November 13, after learning the alarming results of forensic
27 investigation, Poly informed Cisco that it inexplicably intended to return Dr. Chung to his position at
28 Poly the next day, precipitating the filing of the original Complaint on November 18, 2019.

B. Mr. He

1
2 97. Mr. He was an engineer with Cisco, who played an integral role in developing many of
3 Cisco's successful products. Incumbent with Mr. He's responsibilities was access to some of Cisco's
4 most confidential trade secrets used within Cisco's UCTG, including design specifications,
5 schematics, source code, product market analyses, and vendor contract details. Mr. He left Cisco in
6 June 2019 to join Poly.

7 98. Before leaving Cisco, Mr. He, without authorization, willfully and maliciously
8 misappropriated Cisco's confidential and proprietary business information to use for his own benefit,
9 and for the benefit of Poly, to the detriment of Cisco.

10 99. On March 1, 2019, Dr. Chung communicated details of his new position at Poly to Mr.
11 He.

12 100. On March 9, 2019, Dr. Chung told Mr. He that Poly was interested in having Mr. He
13 work there.

14 101. Mr. He regularly took photographs of Cisco Confidential Materials on his iPhone Max.

15 102. For example, on May 13, 2019, Mr. He took a photograph of a financial presentation
16 containing Cisco Confidential Materials, which included Cisco's Q3 financial highlights, largest deals,
17 and comparative revenue by category.

18 103. On May 30, 2019, Mr. He copied Cisco Confidential Materials, including architectural
19 design documents relating to Cisco's unreleased headset concepts to a LaCie external hard drive with
20 serial number 0000NL37HDBX ("LaCie Drive").

21 104. On June 1, 2019, Mr. He traveled from his home in China to California. Mr. He told
22 his manager that this was a personal trip. Mr. He remained in California until June 9, 2019.

23 105. On June 3, 2019, Mr. He took a photo from his iPhone Max of a hardware diagram for
24 a Cisco headset prototype.

25 106. On June 5, 2019, Mr. He took photographs from his iPhone Max of Cisco Confidential
26 Materials that discussed Cisco's emerging business opportunities in the collaboration space. On this
27 date, Mr. He also downloaded a headset test report containing Cisco Confidential Materials.

28 107. On June 6, 2019, Mr. He informed his manager that he was resigning from Cisco.

1 108. On June 6, 2019, Mr. He connected to Cisco's Virtual Private Network from a Comcast
2 IP address in the United States.

3 109. While on Cisco's VPN in the United States on June 6, 2019, Mr. He copied over 100
4 documents to the LaCie Drive. These documents included Cisco Confidential Materials, such as
5 design and configuration documents relating to Cisco's unreleased headset prototypes. Also included
6 in these files was information relating to vendor roadmaps for Cisco's products.

7 110. On June 10, 2019, Mr. He had an in-person meeting with his manager in China. In this
8 meeting, Mr. He discussed his resignation with his manager. Mr. He stated that he was not going to
9 Poly, but that he was moving to Guangzhou for family reasons.

10 111. On June 11, 2019, Mr. He copied an email archive from his Cisco email account to the
11 LaCie Drive. On June 14, 2019, Mr. He copied two additional archives from his Cisco email account
12 to the LaCie Drive. These archives contain Cisco Confidential Materials. Discussions over email
13 contained in the archive reflect Cisco's strategic product development decisions. The email archives
14 also include, as email attachments, technical design documents and presentations containing Cisco's
15 trade secrets.

16 112. On June 17, 2019, Mr. He copied approximately 200 emails from his Cisco email trash
17 folder to the LaCie Drive. These emails contain Cisco Confidential Materials and relate to design
18 details for a then unreleased IP telephone project.

19 113. On June 18, 2019, Mr. He copied approximately 1500 files to the LaCie Drive. These
20 files contain Cisco Confidential Materials and include internal emails, architectural documents,
21 marketing plans, and cost information.

22 114. On June 20, 2019, Mr. He copied approximately 90 files to the LaCie Drive. These
23 files contain Cisco Confidential Materials and relate to Cisco's headset projects.

24 115. On June 21, 2019, Mr. He left Cisco. Mr. He retained the LaCie Drive.

25 116. Mr. He's exfiltration of Cisco Confidential Materials was outside the scope of his
26 employment at Cisco.

27 117. On information and belief, Mr. He joined Poly on or around June 24, 2019.
28

1 118. On June 27, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
2 Drive, including a schematic for an unreleased IP telephone project. Mr. He again accessed this file
3 on July 3, 2019.

4 119. On July 1, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
5 Drive, including a vendor's roadmap update created for Cisco.

6 120. On July 15, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
7 Drive, including a full engineering specification for a next-generation conference room collaboration
8 device. Mr. He had previously copied this file to the LaCie Drive on May 30, 2019.

9 121. On information and belief, Mr. He accessed these Cisco Confidential Materials for his
10 own benefit, and for the benefit of Poly, to Cisco's detriment.

11 122. On August 2, 2019, counsel for Cisco put Mr. He on notice to preserve all documents
12 and things related to the potential misappropriation of Cisco's confidential and proprietary business
13 information.

14 123. On August 5, 2019, after receiving the preservation notice, Mr. He took steps to conceal
15 his misappropriation, including destroying evidence of his unlawful conduct. By way of example, on
16 August 5, Mr. He deleted thousands of Cisco files containing Cisco Confidential Materials from the
17 LaCie Drive. On information and belief, Mr. He deleted these files because Poly had commenced an
18 internal investigation into the misappropriation, and Mr. He was requested to turn the LaCie Drive to
19 Poly's investigators. In addition to the aforementioned files and file types, Mr. He deleted various
20 source code library stacks from the LaCie Drive.

21 124. On August 2, 2019, Cisco notified Poly that Mr. He had misappropriated Cisco
22 Confidential Materials. Poly investigated Cisco's allegations and terminated Mr. He's employment
23 with Poly shortly thereafter.

24 125. Mr. He understood that his employment by Cisco created a relationship of confidence
25 and trust with respect to confidential and proprietary information.

26 126. By the terms of Mr. He's Proprietary Information and Inventions Agreement ("He
27 PIIA"), Mr. He agreed that he would "not remove any [Cisco] Documents and Materials from the
28 business premises of [Cisco] or deliver any [Cisco] Documents and Materials to any person or entity

1 outside [Cisco], except as [] required to do in connection with performing the duties of [his]
 2 employment.” Mr. He also agreed that “immediately upon the termination of [his] employment,” he
 3 would “return all [Cisco] Documents and Materials, apparatus, equipment and other physical property,
 4 or any reproductions of such property”

5 **C. Messrs. Williams & Puorro**

6 127. Mr. Williams was a Regional Sales Director in ASP Architectures when he terminated
 7 his employment at Cisco in October 2019. Prior to that, he was a Director in Global Collaboration
 8 Sales, in which he had global responsibility for developing sales and marketing strategies for bringing
 9 Cisco’s suite of collaboration products to market. Mr. Williams started at Cisco in 1998 as a Systems
 10 Engineer II.

11 128. Mr. Puorro is the Executive Vice President and General Manager of Products at Poly.
 12 On information and belief, Mr. Puorro is the Poly executive officer chiefly responsible for its product
 13 development efforts. Mr. Puorro was a Cisco employee from October 2009 until December 2018. Mr.
 14 Puorro served as Vice President of Cisco’s Unified Communications Technology Group from October
 15 2014 until December 2018. Mr. Puorro left Cisco in December 2018, and, on information and belief,
 16 Mr. Puorro joined Poly in January 2019.

17 129. Mr. Williams stored his iPhone messages in his iCloud account. While employed at
 18 Cisco, Mr. Williams synced his iPhone messages from iCloud account to his Cisco laptop, which
 19 saved a local copy of his iPhone messages on his Cisco laptop.

20 130. Beginning in February 2019, Mr. Williams began aggressively pursuing employment
 21 with Poly. Mr. Williams sought out and received the assistance of Mr. Puorro and other third-parties
 22 to advocate for his candidacy at Poly. Mr. Puorro initiated a scheme whereby he would exchange
 23 coaching and advocacy on Mr. Williams’ behalf for confidential details about Cisco’s competitive
 24 business. As part of this scheme, Mr. Williams shared with Mr. Puorro and other Poly executives
 25 information about upcoming organizational restructurings at Cisco before they were announced to
 26 enable Poly’s recruitment of Cisco employees identified by Mr. Williams and Mr. Puorro, essentially
 27 acting as an agent for Poly within Cisco and while being employed and compensated by Cisco.

28 9/11/2019 3:01:17 PM; Mr. Williams: I’m a huge [Cisco Employee] fan - I’ve seen him work
 miracles over the last 15 years. [REDACTED] - that guy is a sales machine

9/11/2019 3:04:03 PM; Poly Executive: Been talking to [Consultant]?

9/11/2019 3:05:20 PM; Mr. Williams: No - but I gave [Cisco Employee] the heads-up about 30 days ago that there was an external job that may be opening up that he should consider if he gets a call. He connected the dots.

9/11/2019 3:06:28 PM; Poly Executive: Got it

* * *

9/12/2019 2:14:12 PM; Mr. Williams: We are going to execute another LR in two weeks

9/12/2019 6:09:57 PM; Mr. Puorro: Nice

9/12/2019 6:10:12 PM; Mr. Williams: [Cisco Employee] and I had another conversation

9/12/2019 6:10:55 PM; Mr. Williams: if you want him - I think you can get him - but it can't be like me - you have to do it quickly. He's got two very real other jobs he's looking at

131. As Mr. Williams grew more desperate for employment with Poly, Mr. Williams shared with Mr. Puorro and other third parties increasingly sensitive Cisco Confidential Materials. For example, in preparation for an interview with Poly, Mr. Williams shared highly confidential and non-public financial information relating to bookings for Cisco's collaboration business with a third-party consultant who, at the time, Mr. Puorro was trying to bring into Poly, and who shortly thereafter began work at Poly. Further still, Mr. Williams eventually revealed details of various Cisco sales and marketing strategies to Poly's highest ranking executives in order to secure employment. In so doing, Mr. Puorro solicited, and Mr. Williams willfully and maliciously shared, Cisco's trade secrets to "inflict pain" upon Cisco. For example, Mr. Williams, while preparing for an interview with Poly, shared a detailed presentation outline that Mr. Williams' intended to deliver to Poly with the third-party consultant, who would later become employed by Poly himself, containing Cisco's sensitive and non-public financial information. On information and belief, Mr. Williams shared this information with Poly's highest ranking executives while interviewing with Poly. Excerpts from this document are seen below:

Good morning!

I'm remain super excited about the opportunity to come work for you [REDACTED]

How are things going for you?

How's the sales meeting?

Based upon our last conversation I thought I'd share with you a couple of additional items:

1. The Mix of our business across Public Sector, Enterprise, Commercial.
2. How I drive the RTM each and every day with though our channel partners:
 - a) Working with Channels at Cisco [REDACTED]

[REDACTED] Everything we do [REDACTED]

[REDACTED]
[REDACTED]
I may not have emphasized this during our conversations, and that may be due to the fact that [REDACTED]

3. Some aggressive thoughts on how to take advantage of the market transition and opportunity happening now.
4. References for Jedd

The Mix of the Business:

I thought it would be good to share with you the mix of my business and where I spend the majority of my time when it comes to Collaboration.

Globally: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

Americas: [REDACTED] in revenue broke down across these segments/countries:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

132. Collectively, Mr. Williams, Mr. Puorro, and other senior Poly executives knew that their conduct was unlawful. Indeed, they took steps to conceal their illegal conduct by communicating through their personal email addresses (and not their Poly email, which on information and belief, they use for Poly business) and reverting to live discussions so that the details of their communications would not be discovered, because they did not, in their words, "want to put anything on [t]ext that [they] don't want Cisco to have."

1 133. In February 2019, shortly after Mr. Puorro left Cisco for Poly, Mr. Williams contacted
2 Mr. Puorro to ask about employment opportunities at Poly. Mr. Williams was eager to move on from
3 Cisco, and sought out Mr. Puorro's assistance with the job search.

4 134. Mr. Puorro advocated for Mr. Williams' candidacy at Poly. For example, as soon as
5 Mr. Williams expressed interest in joining Poly, Mr. Puorro spoke favorably of Mr. Williams to a Poly
6 sales executive ("First Poly Executive"). Mr. Puorro's advocacy was effective—the First Poly
7 Executive reached out to Mr. Williams days later and arranged for an in-person interview. Mr. Puorro
8 also secured expedited consideration for Mr. Williams. For example, when he learned that Mr.
9 Williams' interview with the sales executive would not occur until the following week, Mr. Puorro
10 arranged for a high ranking Poly executive ("Second Poly Executive") to contact Mr. Williams
11 personally the next day.

12 135. On March 3-4, 2019, Mr. Williams interviewed with executives at Poly. After the
13 interviews, Mr. Williams immediately reached out to Mr. Puorro to discuss the interviews. Mr.
14 Williams indicated that his total target compensation threw the First Poly Executive "a curve ball" and
15 that Mr. Williams received a "let's stay in touch" message. As he would throughout Mr. Williams'
16 interview process, Mr. Puorro counseled Mr. Williams on how to navigate these interviews and
17 interact with Poly's executives. For example, Mr. Puorro communicated to Mr. Williams that
18 compensation is just a decision point, and that he should follow up with the Second Poly Executive in
19 a couple of days. Mr. Puorro maintained regular contact and ensured that Mr. Williams was following
20 his guidance.

21 136. On information and belief, Mr. Puorro provided guidance to Mr. Williams and
22 advocacy for his candidacy within Poly to secure Mr. Williams as a source within Cisco for Cisco
23 Confidential Materials. Mr. Puorro regularly requested confidential details of Cisco's business from
24 Mr. Williams. These requests escalated in sensitivity, and frequently coincided with times when Mr.
25 Puorro's advocacy would be most beneficial to Mr. Williams. On information and belief, Mr. Puorro
26 traded upon Mr. Williams' desperation for a senior position at Poly and his own apparent ability to
27 expedite consideration to induce Mr. Williams to reveal Cisco's trade secrets. Early on in the
28 recruitment process, Mr. Puorro tested Mr. Williams' willingness to reveal sensitive information.

1 137. On March 6, 2019, while Mr. Williams was in San Diego, California, Mr. Puorro asked
 2 Mr. Williams if “org changes” had happened at Cisco. Mr. Williams provided a detailed response.
 3 After Mr. Williams provided these details, he explained that he was ready to move on from Cisco.
 4 Mr. Puorro reassured him that the Second Poly Executive would promptly respond to Mr. Williams’
 5 requests for employment.

6 138. Mr. Puorro would use Poly’s protracted recruitment procedures to his advantage in
 7 inducing Mr. Williams to reveal Cisco Confidential Materials. On information and belief, Mr. Puorro
 8 would present delays as opportunities to advocate on Mr. Williams’ behalf, with the understanding
 9 that Mr. Williams would provide sensitive details about Cisco’s business in return.

10 139. For example, on March 7, 2019, Mr. Puorro informed Mr. Williams that another
 11 individual already had the position Mr. Williams was seeking at Poly. Mr. Puorro asked Mr. Williams
 12 for some time to work with the Second Poly Executive to bring Mr. Williams to Poly.

13 140. Apparently in response, and desperate to prove his usefulness to Poly, on the following
 14 day, March 8, 2019, Mr. Williams provided information to Mr. Puorro about organizational changes
 15 at Cisco. Mr. Puorro requested further details, and on information and belief, Mr. Williams provided
 16 such details.

17 141. On March 13, 2019, less than a week after Mr. Puorro told Mr. Williams that he would
 18 work to bring him into Poly and knowing that Mr. Puorro was interested in learning about
 19 “organization changes” at Cisco before they were made public, Mr. Williams communicated to Mr.
 20 Puorro that he had access to, and was willing to share, the names of individuals who would be impacted
 21 by upcoming organizational changes and encouraged Mr. Puorro that now was the time to act to disrupt
 22 Cisco (dubbed “Project x”):

23 3/11/2019 2:35:32 PM; Mr. Puorro: talk?

24 3/11/2019 2:36:12 PM; Mr. Williams: Yes sir

25 3/13/2019 5:35:31 PM; Mr. Williams: Time is now to recruit. Let’s execute a project x like we did
 with [another company.]

26 3/13/2019 5:35:42 PM; Mr. Williams: I have a list

27 142. On March 18, 2019, Mr. Puorro informed Mr. Williams that he had spoken to the
 28 Second Poly Executive about Mr. Williams, and Mr. Puorro asked to meet with Mr. Williams. Mr.

1 Puorro and Mr. Williams met in person the next day to discuss Mr. Williams' potential employment
2 at Poly.

3 143. On March 22, 2019, Mr. Williams communicated highly confidential details about a
4 matter at Cisco, including Cisco's legal strategy, to Mr. Puorro.

5 144. Mr. Puorro, in addition to advocating for Mr. Williams' candidacy, counseling him on
6 how to interact with Poly's other senior executives, and sharing how his candidacy was being
7 perceived at Poly, also conveyed his own importance in the recruitment process to Mr. Williams. For
8 example, Mr. Puorro communicated that it was he and the Second Poly Executive who would get Mr.
9 Williams to Poly, and Mr. Puorro made key introductions for Mr. Williams.

10 145. On April 1, 2019, Mr. Puorro traveled to California for Poly business. On April 2,
11 2019, Mr. Williams traveled to San Jose, California to meet with Mr. Puorro and other Poly employees
12 to further discuss Mr. Williams' potential employment at Poly and, on information and belief, Cisco's
13 collaboration business. Both Mr. Williams and Mr. Puorro stayed in California until April 5, 2019.

14 146. On information and belief, Mr. Puorro offered his assistance in exchange for Mr.
15 Williams revealing increasingly sensitive Cisco Confidential Materials. When Mr. Williams did not
16 offer these materials, Mr. Puorro's advice was terse, insubstantial, or non-existent.

17 147. On April 30, 2019, Mr. Williams was in Santa Cruz, California for interviews with Poly
18 senior executives.

19 148. On May 9, 2019, Mr. Williams relayed details from Cisco's Global Collaboration
20 Quarterly Business Review meeting to Mr. Puorro, and suggested that he could provide information
21 about Cisco in exchange for an offer with Poly:

22 5/9/2019 6:36:00 PM; Mr. Williams: [Cisco Employee] telling everyone you are now the guy at Poly

23 5/9/2019 6:36:09 PM; Mr. Williams: He covered it off at the Global Collab QBR

24 5/9/2019 7:21:47 PM; Mr. Puorro: We need to find out how [Cisco Employee] knew that.

25 5/9/2019 7:21:58 PM; Mr. Puorro: I think we have a leak in our India team. Anyway you can find out?

26 5/9/2019 7:24:00 PM; Mr. Williams: Will do

27 5/9/2019 7:24:08 PM; Mr. Williams: Can you get me an offer letter

28 5/9/2019 7:24:14 PM; Mr. Williams: kidding

1 5/9/2019 8:19:42 PM; Mr. Williams: Ok

2 5/9/2019 8:19:45 PM; Mr. Williams: Have info

3 5/9/2019 8:20:09 PM; Mr. Williams: I'm open the rest of the day in 11 mins - call me when it works

4 5/9/2019 9:22:01 PM; Mr. Puorro: Free?

5 5/9/2019 9:22:09 PM; Mr. Williams: yes sir

6 149. On information and belief, Mr. Williams shared Cisco Confidential Materials with Mr.
7 Puorro over the phone on May 9, 2019.

8 150. Throughout Mr. Williams' interview process with Poly, Mr. Williams consulted with
9 an individual, who was formerly a Cisco Senior Vice President whom Poly was interested in hiring as
10 a consultant ("Consultant") for interview coaching and job transition strategies. Mr. Puorro introduced
11 Consultant to Poly, where he was indeed later employed as a consultant. On information and belief,
12 Mr. Puorro used Mr. Williams' relationship with Consultant as means to bring Cisco Confidential
13 Materials to Poly. On information and belief, Consultant began working for Poly part time on or
14 around July 29, 2019.

15 5/22/2019 10:59:19 PM; Mr. Williams: I'm having dinner with [CONSULTANT] tonight

16 5/22/2019 10:59:51 PM; Mr. Williams: Let me know if you want me to pass on anything

17 151. On May 25, 2019, on information and belief, Mr. Williams shared Cisco Confidential
18 Materials with Mr. Puorro. "I have something you probably want to know." Mr. Williams said "Just
19 ring me when you can sneak away - don't want to put this one in writing."

20 152. Mr. Williams had an interview scheduled with a Poly executive on June 12, 2019.

21 153. In preparation for the June 12 interview, Mr. Williams prepared a document containing
22 talking points and a job transition strategy. This document indicated that Mr. Williams intended to
23 share with Poly highly confidential and non-public financial data related to Cisco's collaboration
24 business that is directly competitive with Poly. Specifically, the document included a breakdown of
25 bookings data from Cisco's global collaboration business and the growth rate of Cisco's collaboration
26 business. Moreover, the document provided a geographic breakdown of Cisco's global collaboration
27 business, and identified the growth rate of each geographic constituent. The document also further
28 broke down the largest geographic category by segment and country, and provided corresponding

1 growth rates for each segment/country. The document also explained why Cisco's sales to various
2 market segments were increasing or decreasing, and the strategies Cisco employed to secure this
3 growth. The document further described a Cisco sales strategy named "Project Liberator." On June
4 11, 2019, Mr. Williams emailed this market and strategy data outside of Cisco to Consultant, who Mr.
5 Williams knew was not authorized by Cisco to have access to Cisco Confidential Materials.

6 154. The market and strategy data that Mr. Williams sent to Consultant is a compilation of
7 Cisco's confidential financial and business information that is not publicly available, that Cisco has
8 taken reasonable measures to keep secret, and that derives independent economic value from not being
9 generally known to, and not being readily ascertainable through proper means by, another person who
10 can obtain economic value from the disclosure or use of the information.

11 155. On information and belief, Mr. Williams shared Cisco's market and strategy data with
12 Poly at the June 12 interview. During or immediately after the June 12 interview, Poly invited Mr.
13 Williams to an additional round of executive interviews in California on June 28, 2019. Mr. Williams
14 accepted the invitation, and flew to San Francisco, California on June 28, 2019.

15 156. In preparation for the June 28 interviews, Mr. Williams prepared a "discussion guide"
16 PowerPoint presentation. This presentation contained Mr. Williams' plans for accelerating sales at
17 Poly, which included Cisco's product strategy and other financial data, with the admonition that "Poly
18 has to be on Par with Cisco." Mr. Williams later emailed a version of this presentation to Second Poly
19 Executive at the executive's personal email address as opposed to the executive's Poly email.

20 157. Information concerning Cisco's product strategies and other financial data are forms of
21 business information that are not publicly available, that Cisco has taken reasonable measures to keep
22 secret, and that derive independent economic value from not being generally known to, and not being
23 readily ascertainable through proper means by, another person who can obtain economic value from
24 the disclosure or use of the information.

25 158. On June 28, 2019, before Mr. Williams was to interview with Poly executives, Mr.
26 Puorro contacted Mr. Williams to inquire about a potential Limited Restructuring ("LR"), including
27 layoffs, in Cisco's Collaboration Business Unit ("BU"). Mr. Puorro stated "I heard more LR in the
28 BU's Wonder if [Cisco Employee] is safe or not." Mr. Puorro asked Mr. Williams to "Dig for

1 me?” On information and belief, Mr. Williams investigated on behalf of Mr. Puorro and provided
2 details on the magnitude of the potential LR.

3 159. Information concerning Cisco’s potential LR’s is a form of business information that
4 is not publicly available, that Cisco has taken reasonable measures to keep secret, and that derives
5 independent economic value from not being generally known to, and not being readily ascertainable
6 through proper means by, another person who can obtain economic value from the disclosure or use
7 of the information.

8 160. On July 1, 2019, Mr. Puorro asked Mr. Williams if Cisco had performed the potential
9 LR yet. Mr. Williams provided a detailed response.

10 161. Between July 1 and August 19, Mr. Williams contacted Mr. Puorro more than 20 times
11 concerning the potential employment opportunity at Poly. Mr. Puorro provided only terse responses
12 suggesting that he was too busy to discuss the potential employment opportunity for Mr. Williams at
13 Poly.

14 162. On July 31, 2019, Mr. Williams sent a message to Second Poly Executive in which Mr.
15 Williams proposed that it was “[t]ime to execute Project Liberator while Cisco is further distracted,
16 grow sales and gain marketshare.” Project Liberator is an ongoing Cisco sales strategy that Mr.
17 Williams was involved with developing and executing while at Cisco. The specific details and tactics
18 of Project Liberator are Cisco Confidential Materials.

19 163. On August 19, 2019, Mr. Williams told Mr. Puorro about two individuals who had just
20 left Cisco. Mr. Williams gave Mr. Puorro the names of additional people that Mr. Williams believed
21 Mr. Puorro could recruit to Poly.

22 164. On August 22, 2019, Mr. Williams sent an email to Second Poly Executive’s personal
23 gmail account describing his vision for executing “Project x” at Poly. Project x is a Cisco sales strategy
24 that Mr. Williams was involved with developing and executing while at Cisco. The specific details
25 and tactics of Project x are Cisco Confidential Materials. Mr. Williams discussed Project x with
26 Second Poly Executive. The Second Poly Executive asked Mr. Williams to connect with Mr. Puorro
27 and yet another Poly executive (“Third Poly Executive”) to “figure out next steps to execute the
28

1 concept” Mr. Williams subsequently shared the details of Project x with Mr. Puorro and Third
2 Poly Executive.

3 165. On August 27, 2019, Mr. Williams informed Mr. Puorro about Cisco’s investment in
4 an emerging technology. Mr. Puorro then asked Mr. Williams about an internal Cisco meeting:

5 8/27/2019 6:58:32 PM; Mr. Puorro: How was UC break out yesterday?

6 8/27/2019 7:05:20 PM; Mr. Williams: Just got to my room if you want to chat

7 8/27/2019 7:05:32 PM; Mr. Puorro: Getting on plane..

8 8/27/2019 7:06:09 PM; Mr. Williams: Sounds good - ping me later - don’t want to put anything
9 on Text that I don’t want Cisco to have!

10 166. Upon information and belief, Mr. Williams later orally provided Cisco Confidential
11 Materials about the internal Cisco meeting to Mr. Puorro.

12 167. On August 28, 2019, Mr. Williams shared pictures from this internal meeting with Mr.
13 Puorro. These pictures contained Cisco’s screenshots of presentations and an image of a new Cisco
14 headset. Mr. Williams communicated to Mr. Puorro that he was “so ready to show [Cisco] that Poly
15 can inflict pain.” Mr. Williams referred to Cisco’s upcoming products by stating “They’ve got some
16 good [expletive] coming.” Mr. Puorro asked “[d]oes it work with Zoom.” On information and belief,
17 Mr. Williams’ response reflected Cisco Confidential Information shared at the internal meeting. Mr.
18 Williams also provided Mr. Puorro with details from a presentation at this Cisco internal meeting,
19 explaining Cisco’s competitive focus.

20 168. On September 3, 2019, Mr. Williams informed Mr. Puorro that he was meeting with a
21 Cisco customer (whom he named), and stated “Looking at them from the Cisco lens. I could easily
22 change that lens though.”

23 169. Upon information and belief, on September 7, 2019, Mr. Puorro solicited Cisco
24 Confidential Materials from Mr. Williams. Mr. Puorro and Mr. Williams had a conversation during
25 which Mr. Williams communicated Cisco Confidential Materials to Mr. Puorro.

26 9/7/2019 2:42:47 PM; Mr. Puorro: I’m curious how is my old [REDACTED] product doing?

27 9/7/2019 2:43:31 PM; Mr. Williams: I asked that very question earlier this week

28 9/7/2019 2:43:41 PM; Mr. Williams: REDACTED

1 9/7/2019 2:44:51 PM; Mr. Puorro: I think [REDACTED] tries to kill it

2 9/7/2019 2:45:07 PM; Mr. Williams: Talk ?

3 9/7/2019 2:46:04 PM; Mr. Williams: Just in case big brother is watching...

4 9/7/2019 2:46:42 PM; Mr. Puorro: Calling

5
6 170. On September 12, 2019, Mr. Williams notified Mr. Puorro that he had turned down a
7 job offer from another company, and that he hoped to hear something from Poly that day. He then
8 revealed details about a prospective Cisco LR, and identified a Cisco employee for Poly to recruit.

9 171. On September 13, 2019, Mr. Williams told Mr. Puorro that he had heard Poly was
10 “having hell with Cisco legal,” apparently a reference to Cisco’s communication with Poly’s General
11 Counsel regarding Dr. Chung and Mr. He. Mr. Puorro stated “we are past that I believe.” Mr. Williams
12 said “They aren’t going to give two [expletive] about me with where I’m at now.” Mr. Williams then
13 told Mr. Puorro that he had “interesting rumors” about Cisco and Collaboration and wished to speak
14 with Mr. Puorro live. Mr. Puorro called Mr. Williams minutes later.

15 172. Also, on September 16, 2019, Mr. Williams communicated with Mr. Puorro and Third
16 Poly Executive about Project x. Mr. Williams conveyed to Second Poly Executive that these were
17 “Great conversations” and asked Second Poly Executive if anything further was required.

18 173. On September 17, Second Poly Executive said that he would get the HR people “in
19 gear today.” Second Poly Executive asked Poly’s human resources department to move fast.

20 174. On September 18, 2019, Mr. Williams notified Mr. Puorro of a prospective LR at Cisco.
21 Mr. Williams also provided details concerning the status of a Cisco business unit, and identified an
22 employee potentially impacted by the LR who he believed could be recruited by Poly.

23 175. On information and belief, on September 19, 2019, Mr. Williams was informed an
24 employment offer at Poly would be forthcoming.

25 176. Mr. Williams received a formal employment offer to join Poly on September 26, 2019.

26 177. Information concerning Cisco’s investments in emerging technologies, Cisco’s
27 competitive focus, Cisco’s sales opportunities and customer lists, Cisco’s new products, and Cisco’s
28 future plans for its current products are forms of business information that are not publicly available,

1 that Cisco has taken reasonable measures to keep secret, and that derives independent economic value
2 from not being generally known to, and not being readily ascertainable through proper means by,
3 another person who can obtain economic value from the disclosure or use of the information.

4 178. On October 10, 2019, Mr. Williams received his Poly network credentials.

5 179. On October 11, 2019, Mr. Williams received from Poly his first week schedule, with a
6 planned start date of October 14, 2019.

7 180. On October 12, 2019, Mr. Williams signed a Poly form certifying that he had not
8 downloaded onto any device any of Cisco's confidential information. Mr. Williams also certified that
9 Cisco had reviewed and/or deleted, or that he had deleted, any of Cisco's confidential information.
10 Mr. Williams also certified that he had returned all of Cisco's equipment and property to Cisco.

11 181. Mr. Williams October 12, 2019 certification was false. On information and belief, Poly
12 knew, or was willfully blind to the fact, that Mr. Williams was still employed at Cisco at the time of
13 the certification and had access to and possession of Cisco Confidential Materials and equipment. For
14 example, Mr. Williams indicated to Poly's human resources department that he would like to begin
15 regular work activities on October 15, because of issues with Cisco's human resources department.

16 182. Mr. Williams traveled to Santa Clara, California on October 13, 2019.

17 183. After receiving and accepting Poly's offer of employment, Mr. Williams requested a
18 monetary separation package from Cisco. Even though he was directly asked during these discussions
19 about his plans after leaving Cisco, Mr. Williams claimed that he was going to work at his church and
20 focus on personal issues. In light of these circumstances and to help Mr. Williams with his family,
21 Cisco offered Mr. Williams two months sales pay, in addition to a lump sum payment to cover two
22 months COBRA health care premiums. At the time, Mr. Williams of course already had accepted an
23 offer with Poly, which included health benefits.

24 184. Mr. Williams returned his laptop to Cisco's San Jose office in person. Mr. Williams
25 was obligated by Cisco to return all other Cisco Confidential Materials he possessed at that time.

26 185. Mr. Williams' employment with Cisco terminated on October 15, 2019.

27 186. Mr. Williams' disclosures of Cisco Confidential Information to Mr. Puorro were
28 outside the scope of his employment at Cisco.

1 187. During the course of his employment at Cisco, Mr. Williams ran a home server that he
2 used to store a Time Machine backup of his Cisco laptop. This backup contained, and, on information
3 and belief, still contains Cisco Confidential Materials, including detailed information about Cisco's
4 sales forecasts and opportunities, including customer names, commitments, and upsides. Mr. Williams
5 did not return this backup to Cisco upon his termination. Mr. Williams' retention of this backup was
6 outside the scope of his employment at Cisco.

7 **D. Poly**

8 188. Paragraphs 1 through 187 are incorporated by reference as if fully stated herein.

9 189. Poly acquired and used Cisco's trade secrets through the actions of its employee, Dr.
10 Chung. For example, Dr. Chung accessed Cisco Confidential Materials that he misappropriated at
11 least on February 26, March 8, and March 24, 2019 while he was employed at Poly. On information
12 and belief, Dr. Chung used these Cisco Confidential Materials within the course and scope of his
13 employment at Poly. The Cisco Confidential Materials accessed by Dr. Chung while he was employed
14 at Poly contain Cisco's trade secrets.

15 190. On September 9, 2019, Cisco notified Poly through its General Counsel that Dr. Chung
16 had misappropriated Cisco Confidential Materials. Poly did not place Dr. Chung on administrative
17 leave at this time, and, on information and belief, took no action adverse to Dr. Chung. Having not
18 heard back from Poly, Cisco followed up on September 17, 2019, to reiterate its concerns about Dr.
19 Chung. Poly's General Counsel stated that Dr. Chung denied taking any of Cisco Confidential
20 Materials. On September 26, 2019, Poly wrote to Cisco and provided follow up information which
21 confirmed that Dr. Chung's representations to Poly were false. Indeed, Dr. Chung had, in fact, taken
22 Cisco Confidential Materials to Poly, including at least the EA Document and Webex Vision
23 Document. Despite his dishonesty, Poly still took no action adverse to Dr. Chung. On October 9,
24 2019, Cisco again contacted Poly about its concerns with Dr. Chung, and also provided Poly with
25 information confirming that Dr. Chung's explanation for the whereabouts of the First Seagate Drive
26 and Second Seagate Drive was not credible. Only then did Poly place Dr. Chung on a brief
27 administrative leave. Cisco and Poly then arranged for Dr. Chung's devices to be analyzed by a third
28 party. Dr. Chung did not turn over the First Seagate Drive or the Second Seagate Drive for analysis.

1 The forensic investigation revealed that Dr. Chung accessed Cisco Confidential Materials after the
2 start of his employment with Poly, that he emailed Cisco Confidential Materials to his Poly email
3 address, and that apparent data wiping procedures were performed on at least the Sandisk and Samsung
4 Drives after Cisco requested Dr. Chung to preserve all data. The third party forensics lab reported
5 these results to Poly. The whereabouts of the First Seagate Drive and Second Seagate Drive, which
6 contain Cisco Confidential Materials, remain unknown to Cisco, and, on information and belief, to
7 Poly. Nevertheless, on the evening of November 13, Poly informed Cisco that it inexplicably intended
8 to return Dr. Chung to his position the very next day.

9 191. On October 18, 2019, when the severity and gravity of Dr. Chung and Mr. He's
10 misappropriation became clear to Poly, Poly's General Counsel raised allegations (later proved to be
11 unsupported) that a former Poly employee who had recently joined Cisco exfiltrated confidential Poly
12 materials on a thumb drive. On information and belief, Poly raised these allegations as a tactical
13 maneuver to compel Cisco to cease its investigations into Dr. Chung and Mr. He. Cisco immediately
14 placed this employee on administrative leave and performed a thorough investigation. Cisco's
15 investigation revealed that Poly's claims had no merit. When Cisco revealed the results of its
16 investigation, Poly did not challenge the results. Rather, Poly raised an additional allegation against
17 this same employee that Cisco investigated and found was not credible.

18 192. Poly knew or should have known that Dr. Chung still possessed, and intended to use in
19 his employment at Poly, Cisco Confidential Materials when it permitted him to return to work on
20 November 14, 2019.

21 193. Poly ratified Dr. Chung's misappropriation of Cisco's trade secrets by failing to
22 terminate his employment after discovering that he had, in fact, misappropriated Cisco Confidential
23 Materials.

24 194. Poly also ratified Dr. Chung's misappropriation of Cisco's trade secrets by permitting
25 him to return to work when it knew or should have known that Dr. Chung still possessed Cisco
26 Confidential Materials.

27 195. Poly also acquired and used Cisco's trade secrets through the actions of its former
28 employee, James He. For example, Mr. He accessed Cisco Confidential Materials that he

1 misappropriated on June 27, July 1, and July 15, 2019 while he was employed at Poly. On information
2 and belief, Mr. He used these Cisco Confidential Materials within the course and scope of his
3 employment at Poly. The Cisco Confidential Materials accessed by Mr. He while he was employed
4 at Poly contain Cisco's trade secrets.

5 196. Poly also acquired through improper means, and on information and belief, used
6 Cisco's trade secrets through the actions of its officer, Mr. Puorro. Mr. Puorro acted in concert with
7 Mr. Williams to acquire and use Cisco Confidential Materials at Poly. On information and belief,
8 Poly's executives were aware of Mr. Puorro's conduct, and acquiesced to it. Poly's executives,
9 including at least Second Poly Executive and Third Poly Executive knew or should have known that
10 Mr. Williams was revealing Cisco Confidential Materials to Mr. Puorro, at least because Mr. Williams
11 shared details relating to Project x, including that it was a Cisco project, to the Second Poly Executive
12 and Third Poly Executive. Furthermore, Mr. Puorro's inducement of Mr. Williams to disclose Cisco
13 trade secrets to him and others at Poly was within the course and scope of Mr. Puorro's employment
14 at Poly and was intended to benefit Poly to the detriment of Cisco.

15 **COUNT I**

16 **Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Dr. Chung**

17 197. Paragraphs 1 through 196 are incorporated by reference as if fully stated herein.

18 198. Dr. Chung's misappropriation of trade secrets is actionable under the Defend Trade
19 Secrets Act, 18 U.S.C. § 1836.

20 199. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For
21 example, these trade secrets include Cisco technical information such as source code, schematics,
22 design details and specifications, user feedback, design documentation, and features relating to Cisco's
23 existing and future products, as well as Cisco business information such as marketing strategy, cost
24 and pricing information, and payment information.

25 200. Dr. Chung misappropriated Cisco's trade secrets by improper means (including, for
26 example, by systematically transferring Cisco Confidential Materials out of Cisco immediately
27 preceding his departure), by disclosure without authorization (including, for example, by uploading
28

1 Cisco Confidential Materials to Poly's Sharepoint site), and by use without authorization (including,
2 for example, to obtain a competitive advantage in his product development efforts).

3 201. Dr. Chung has maintained and continues to maintain in his possession the wrongfully
4 acquired Cisco documents and materials after the termination of his employment with Cisco.

5 202. Dr. Chung used and continues to use Cisco trade secret contained in these wrongfully
6 acquired Cisco documents by way of providing these documents to Poly and/or accessing these
7 documents.

8 203. Dr. Chung's possession after leaving Cisco, acquisition, disclosure, and/or use of Cisco
9 trade secrets was and is without Cisco's express or implied consent.

10 204. Cisco trade secrets were developed over time after expenditure of significant effort and
11 resources.

12 205. Cisco trade secrets are not publicly available, and are kept within the knowledge and
13 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
14 bound by contractual obligations of confidentiality.

15 206. Cisco has taken reasonable measures to keep its trade secret information secret.

16 207. Cisco communicates the importance of maintaining confidentiality to its employees in
17 various means and forms, including but not limited to the Proprietary Information and Inventions
18 Agreements and termination letters.

19 208. On February 9, 2007, Dr. Chung executed the Chung PIIA in consideration for his
20 employment with Cisco.

21 209. The Chung PIIA protects Cisco's proprietary information, which was defined in the
22 Chung PIIA as (i) information that was or will be developed, created, or discovered by or on behalf of
23 Cisco, or which became or will become known by, or was or is conveyed to Cisco, which has
24 commercial value in Cisco's business, or (ii) any other information that Cisco does not want publicly
25 disclosed. The Chung PIIA further states that Cisco proprietary information includes but is not limited
26 to software programs and subroutines, source and object code, algorithms, trade secrets, designs,
27 technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or not),
28 works of authorship, formula, business and product development plans, customer lists, terms of

1 compensation and performance levels of Cisco employees, and other information concerning Cisco's
2 actual or anticipated business, research or development, or which is received in confidence by or for
3 Cisco from any other source, or any document that is marked as "confidential."

4 210. By signing the Chung PIIA, Dr. Chung agreed that he would "not remove any Company
5 Documents and Materials from the business premises of Cisco or deliver any Company Documents
6 and Materials to any person or entity outside of Cisco, except as [] required to do in connection with
7 performing the duties of [his] employment." Dr. Chung also agreed that "immediately upon the
8 termination of [his] employment," he would "return all Company Documents and Materials, apparatus,
9 equipment and other physical property, or any reproductions of such property"

10 211. Dr. Chung took intentional and systematic steps during at least a three and a half week
11 period before the termination of his employment to transfer thousands of documents containing Cisco
12 Confidential Materials out of Cisco.

13 212. Upon termination of Dr. Chung's employment at Cisco on February 18, 2019, Cisco
14 delivered to Dr. Chung a termination letter, reminding Dr. Chung of his continuing obligations to
15 Cisco, including the duty to maintain confidentiality of Cisco confidential information, the duty of
16 non-solicitation within one year after the termination of Dr. Chung's employment, and the duty to
17 return any Cisco documents as soon as possible.

18 213. Dr. Chung did not return the Cisco Confidential Materials that he had systematically
19 transferred out of Cisco.

20 214. Cisco implements security measures such as electronic access points to restrict access
21 to Cisco's confidential and proprietary information.

22 215. Cisco trade secrets derive independent economic value, actual or potential, from not
23 being generally known to, and/or not being readily ascertainable through proper means by, the public
24 or other persons who can obtain economic value from the disclosure or use of the information.

25 216. Cisco's trade secrets at issue in this case are related to products that are placed in or are
26 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
27 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
28 1836.

COUNT III**Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. He**

227. Paragraphs 1 through 226 are incorporated by reference as if fully stated herein.

228. Mr. He's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

229. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco technical information such as design and architectural documents, hardware diagrams, schematics, source code stacks, and engineering specification relating to existing and future Cisco products, as well as business information such as relating to marketing plans, business opportunities, and revenue and cost information that is not disclosed in publicly available financial reports.

230. Mr. He's misappropriated Cisco's trade secrets by improper means (including, for example, by systematically transferring Cisco Confidential Materials out of Cisco immediately preceding his departure), on information and belief by disclosure without authorization, and by use without authorization (including, for example, to obtain a competitive advantage in his product development efforts).

231. Mr. He maintained in his possession these wrongfully acquired Cisco documents and materials after the termination of his employment with Cisco.

232. On information and belief, Mr. He has used Cisco trade secrets contained in these wrongfully acquired Cisco documents.

233. Mr. He's possession after leaving Cisco, acquisition, disclosure, and/or use of Cisco trade secrets was and is without Cisco's express or implied consent.

234. Cisco trade secrets were developed over time after expenditure of significant effort and resources.

235. Cisco trade secrets are not publicly available, and are kept within the knowledge and know-how of Cisco employees under strict confidentiality obligations, and only shared with parties bound by contractual obligations of confidentiality.

236. Cisco has taken reasonable measures to keep its trade secret information secret.

1 237. Cisco communicates the importance of maintaining confidentiality to its employees in
2 various means and forms, including but not limited to the Proprietary Information and Inventions
3 Agreements and termination letters.

4 238. On March 8, 1999, Mr. He executed the He PIIA in consideration for his employment
5 with Cisco.

6 239. The He PIIA protects Cisco's proprietary information, which was defined in the He
7 PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or which
8 became or will become known by, or was or is conveyed to Cisco, which has commercial value in
9 Cisco's business. The He PIIA further states that Cisco proprietary information includes but is not
10 limited to software programs and subroutines, source and object code, algorithms, trade secrets,
11 designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or
12 not), works of authorship, formula, business and product development plans, customer lists, terms of
13 compensation and performance levels of Cisco employees, and other information concerning Cisco's
14 actual or anticipated business, research or development, or which is received in confidence by or for
15 Cisco from any other person.

16 240. By signing the He PIIA, Mr. He agreed that he would "not remove any Company
17 Documents and Materials from the business premises of [Cisco] or deliver any Company Documents
18 and Materials to any person or entity outside [Cisco], except as [] required to do in connection with
19 performing the duties of [his] employment." Mr. He also agreed that "immediately upon the
20 termination of [his] employment," he would "return all Company Documents and Materials, apparatus,
21 equipment and other physical property, or any reproductions of such property"

22 241. Mr. He took intentional and systematic steps at least during a six week period before
23 the termination of his employment to transfer thousands of documents containing Cisco Confidential
24 Materials out of Cisco.

25 242. Cisco implements security measures such as electronic access points to restrict access
26 to Cisco's confidential and proprietary information.

243. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

244. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

245. Defendant Mr. He's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

246. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

247. On information and belief, if Defendant Mr. He's conduct is not remedied and/or enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's detriment Cisco's trade secret information.

248. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Mr. He's continued misappropriation of Cisco's trade secret information.

COUNT IV

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. He

249. Paragraphs 1 through 248 are incorporated by reference as if fully stated herein.

250. Mr. He's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 et seq.

251. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

252. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

253. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

254. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

255. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT V

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. Williams

256. Paragraphs 1 through 255 are incorporated by reference as if fully stated herein.

257. Mr. Williams' misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

258. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's market and strategy data, partner margins, potential limited restructurings, information concerning Cisco's emerging technologies, competitive focus, sales opportunities and customer lists, product pipelines, and future plans for current products. On information and belief, the Cisco documents stored on Mr. Williams' server backup include Cisco's trade secrets such as customer lists, pricing information and strategic business development plans.

259. Mr. Williams misappropriated Cisco's trade secrets by acquisition by improper means (including, for example, by retaining possession of Cisco Confidential Materials after the termination of his employment), by disclosure without authorization (including, for example, by disclosing Cisco Confidential Materials to Mr. Puorro, to other Poly executives, and to Consultant), and by use without authorization (such as to obtain a competitive business advantage in sales and marketing).

1 260. Mr. Williams' possession after leaving Cisco, acquisition, disclosure, and/or use of
2 Cisco trade secrets was and is without Cisco's express or implied consent.

3 261. Cisco trade secrets were developed over time after expenditure of significant effort and
4 resources.

5 262. Cisco trade secrets are not publicly available, and are kept within the knowledge and
6 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
7 bound by contractual obligations of confidentiality.

8 263. Cisco has taken reasonable measures to keep its trade secret information secret.

9 264. Cisco communicates the importance of maintaining confidentiality to its employees in
10 various means and forms, including but not limited to the Proprietary Information and Inventions
11 Agreements and termination letters.

12 265. On July 20, 1998, Mr. Williams executed the Williams PIIA in consideration for his
13 employment with Cisco.

14 266. The Williams PIIA protects Cisco's proprietary information, which was defined in the
15 Williams PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or
16 which became or will become known by, or was or is conveyed to Cisco, which has commercial value
17 in Cisco's business. The Williams PIIA further states that Cisco proprietary information includes but
18 is not limited to software programs and subroutines, source and object code, algorithms, trade secrets,
19 designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or
20 not), works of authorship, formula, business and product development plans, customer lists, terms of
21 compensation and performance levels of Cisco employees, and other information concerning Cisco's
22 actual or anticipated business, research or development, or which is received in confidence by or for
23 Cisco from any other person.

24 267. By signing the Williams PIIA, Mr. Williams agreed that he would "keep in confidence
25 and trust and will not use or disclose any Proprietary Information of anything relating to it without the
26 prior written consent of an officer of the company, except as may be necessary in the ordinary course
27 of perming my duties to the Company." Mr. Williams also agreed that he would "not remove any
28 Company Documents and Materials from the business premises of [Cisco] or deliver any Company

1 Documents and Materials to any person or entity outside [Cisco], except as [] required to do in
2 connection with performing the duties of [his] employment.” Mr. Williams also agreed that
3 “immediately upon the termination of [his] employment,” he would “return all Company Documents
4 and Materials, apparatus, equipment and other physical property, or any reproductions of such
5 property”

6 268. Before leaving Cisco, Mr. Williams took intentional steps to transfer Cisco
7 Confidential Materials out of Cisco.

8 269. Cisco implements security measures such as electronic access points to restrict access
9 to Cisco’s confidential and proprietary information.

10 270. Cisco trade secrets derive independent economic value, actual or potential, from not
11 being generally known to, and/or not being readily ascertainable through proper means by, the public
12 or other persons who can obtain economic value from the disclosure or use of the information.

13 271. Cisco’s trade secrets at issue in this case are related to products that are placed in or are
14 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
15 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
16 1836.

17 272. Defendant Mr. Williams’ misappropriation of Cisco’s trade secret information was
18 willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. §
19 1836(b)(3)(C) and its attorneys’ fees and costs under 18 U.S.C. § 1836(b)(3)(D).

20 273. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

21 274. On information and belief, if Defendant Mr. Williams’ conduct is not remedied and /or
22 enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to
23 Cisco’s detriment Cisco’s trade secret information.

24 275. Because Cisco’s remedy at law is inadequate, Cisco seeks, in addition to damages,
25 preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and
26 trade secret information and other legitimate business interests. Injunctive relief is necessary to
27 eliminate the commercial advantage that otherwise would be derived from Mr. Williams’ continued
28 misappropriation of Cisco’s trade secret information.

COUNT VI

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. Williams

276. Paragraphs 1 through 275 are incorporated by reference as if fully stated herein.

277. Mr. Williams' misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

278. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

279. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

280. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

281. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

282. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code § 3426.2.

COUNT VII

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. Puorro

283. Paragraphs 1 through 282 are incorporated by reference as if fully stated herein.

284. Mr. Puorro's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

285. The materials and information that Mr. Puorro solicited from Mr. Williams contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's market and strategy data, partner margins, potential limited restructurings, information concerning Cisco's

1 emerging technologies, competitive focus, sales opportunities and customer lists, product pipelines,
2 and future plans for current products.

3 286. Mr. Puorro misappropriated Cisco's trade secrets by acquisition by improper means
4 (including, for example, by inducing Mr. Williams to reveal Cisco Confidential Materials), by
5 disclosure without authorization (including, for example, by revealing Cisco Confidential Materials to
6 others at Poly), and by use without authorization (such as to obtain a competitive business advantage
7 in sales, marketing, and product development efforts).

8 287. As a former Cisco employee, Mr. Puorro knew or should have known that Mr. Williams
9 had a duty to maintain secrecy over the materials he induced Mr. Williams to reveal.

10 288. Mr. Puorro's acquisition, disclosure, and/or use of Cisco trade secrets was and is
11 without Cisco's express or implied consent.

12 289. Cisco trade secrets were developed over time after expenditure of significant effort and
13 resources.

14 290. Cisco trade secrets are not publicly available, and are kept within the knowledge and
15 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
16 bound by contractual obligations of confidentiality.

17 291. Cisco has taken reasonable measures to keep its trade secret information secret.

18 292. Cisco communicates the importance of maintaining confidentiality to its employees in
19 various means and forms, including but not limited to the Proprietary Information and Inventions
20 Agreements and termination letters.

21 293. Cisco implements security measures such as electronic access points to restrict access
22 to Cisco's confidential and proprietary information.

23 294. Cisco trade secrets derive independent economic value, actual or potential, from not
24 being generally known to, and/or not being readily ascertainable through proper means by, the public
25 or other persons who can obtain economic value from the disclosure or use of the information.

26 295. Cisco's trade secrets at issue in this case are related to products that are placed in or are
27 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
28

1 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
2 1836.

3 296. Defendant Mr. Puorro's misappropriation of Cisco's trade secret information was
4 willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. §
5 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

6 297. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

7 298. On information and belief, if Defendant Mr. Puorro's conduct is not remedied and /or
8 enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to
9 Cisco's detriment Cisco's trade secret information.

10 299. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages,
11 preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and
12 trade secret information and other legitimate business interests. Injunctive relief is necessary to
13 eliminate the commercial advantage that otherwise would be derived from Mr. Williams' continued
14 misappropriation of Cisco's trade secret information.

15 **COUNT VIII**

16 **Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. Puorro**

17 300. Paragraphs 1 through 299 are incorporated by reference as if fully stated herein.

18 301. Mr. Puorro's misappropriation of trade secrets is independently actionable under
19 California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

20 302. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

21 303. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or
22 reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

23 304. Defendant's misappropriation of Cisco's trade secret information was willful and
24 malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and
25 its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

26 305. On information and belief, if the Defendant's conduct is not remedied, and if the
27 Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their
28 own benefit and to Cisco's detriment Cisco's trade secret information.

Intentional Interference with a Contractual Relationship by Mr. Puorro

308. The Williams PIIA was a written contract between Cisco and Mr. Williams which restricted Mr. Williams from using or disclosing any of Cisco's proprietary information, including secrets, without the prior written consent of an officer of the Company.

309. Mr. Puorro was aware of the Williams PIIA. For example, Mr. Puorro himself signed a Proprietary Information And Invention Agreement (The “Puorro PIIA”) which similarly prohibited the use and disclosure of Cisco’s proprietary information, including trade secrets. Mr. Puorro was also reminded of his obligations under the PIIA as recently as February 2019. As another example, Cisco’s practice of entering Proprietary Information and Inventions Agreements with its employees is well known in the industry generally. As another example, Cisco sent Dr. Chung and Mr. He’s PIIA agreements to Poly during the course of those investigations, and, on information and belief, those letters were shared with Mr. Puorro.

310. Mr. Puorro engaged in conduct that prevented and/or hindered performance of the Williams PIIA, for example, by inducing Mr. Williams to reveal Cisco's proprietary information and trade secrets to Mr. Puorro and other Poly executives.

311. Mr. Puorro intended for Mr. Williams to reveal Cisco's proprietary information and trade secrets or knew it was likely. For example, Mr. Williams repeatedly conveyed his desire for a job at Poly to Mr. Puorro, and Mr. Puorro offered his advocacy in exchange for Mr. Williams' revealing Cisco Confidential Materials. Moreover, Mr. Puorro continued this course of conduct after

1 Mr. Williams first revealed Cisco Confidential Materials, and therefore intended for Mr. Williams'
2 conduct to continue.

3 312. Cisco has been substantially harmed as a proximate result of Mr. Puorro's conduct. For
4 example, Mr. Puorro's intentional interference with the Williams PIIA threatens to damage the value
5 of Cisco's trade secret technology and business processes, and has provided Poly with proprietary
6 information about Cisco's financial performance, customers, internal business processes, and product
7 development plans, which, on information and belief, Poly is using for its own benefit and to the
8 detriment of Cisco.

9 313. Mr. Puorro's actions were willful, intentional, and malicious. Cisco is therefore
10 entitled to punitive and exemplary damages.

11 **COUNT X**

12 **Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Poly**

13 314. Paragraphs 1 through 313 are incorporated by reference as if fully stated herein.

14 315. Poly's misappropriation of trade secrets is actionable under the Defend Trade Secrets
15 Act, 18 U.S.C. § 1836.

16 316. The materials and information that Mr. Puorro solicited from Mr. Williams contained
17 trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's market and
18 strategy data, partner margins, potential limited restructurings, information concerning Cisco's
19 emerging technologies, competitive focus, sales opportunities and customer lists, product pipelines,
20 and future plans for current products. The materials used by Dr. Chung and Mr. He while employed
21 at Poly also included trade secrets, including, for example, non-public design specifications for current
22 and unreleased Cisco products.

23 317. Poly is vicariously liable for the actions of its officer, Mr. Puorro during the course and
24 scope of his employment at Poly. Mr. Puorro misappropriated Cisco's trade secrets by acquisition by
25 improper means (including, for example, by inducing Mr. Williams to reveal Cisco Confidential
26 Materials), by disclosure without authorization (including, for example, by revealing Cisco
27 Confidential Materials to others at Poly), and by use without authorization (such as to obtain a
28 competitive business advantage in sales, marketing, and product development efforts).

1 318. Additional Poly officers were aware of Mr. Puorro's inducement of Mr. Williams, and
2 ratified his conduct on behalf of Poly. For example, at least one other Poly officer was aware of Mr.
3 Puorro's inducement of Mr. Williams to disclose Cisco Confidential Material to others at Poly. That
4 other Poly officer further ratified Mr. Puorro's conduct on behalf of Poly by requesting that Mr.
5 Williams disclose Cisco Confidential Material to Poly and others at Poly.

6 319. Poly is vicariously liable for the actions of Dr. Chung and Mr. He during the course
7 and scope of their employment at Poly. Dr. Chung misappropriated Cisco's trade secrets by improper
8 means (including, for example, by systematically transferring Cisco Confidential Materials out of
9 Cisco immediately preceding his departure), by disclosure without authorization (including, for
10 example, by uploading Cisco Confidential Materials to Poly's Sharepoint site), and by use without
11 authorization (including, for example, to obtain a competitive advantage in his product development
12 efforts). Dr. Chung further operated within the scope of his employment with Poly when he recruited
13 Mr. He to join Poly. Mr. He's misappropriated Cisco's trade secrets by improper means (including,
14 for example, by systematically transferring Cisco Confidential Materials out of Cisco immediately
15 preceding his departure), on information and belief by disclosure without authorization, and by use
16 without authorization (including, for example, to obtain a competitive advantage in his product
17 development efforts).

18 320. Poly is further liable for Dr. Chung's acts of misappropriation because it ratified Dr.
19 Chung's actions and misappropriation of Cisco's trade secrets when it failed to disavow Dr. Chung's
20 conduct or terminate his employment after Poly had reason to know of Dr. Chung's misappropriation.

21 321. Poly is further liable for Mr. Williams' acts of misappropriation because it ratified Mr.
22 Williams' actions and misappropriation of Cisco's trade secrets when it hired him after Poly had
23 reason to know of Mr. Williams' misappropriation through the actions of its senior executives
24 including Mr. Puorro.

25 322. Upon information and belief, the Poly Executive Officers' familiar with the misconduct
26 of Mr. Puorro and Mr. Williams were also aware of Poly's decisions with respect to Dr. Chung, thus
27 demonstrating an intentional and willful disregard for Cisco's trade secrets by Poly.
28

1 323. Poly's acquisition, disclosure, and/or use of Cisco trade secrets was and is without
2 Cisco's express or implied consent.

3 324. Cisco trade secrets were developed over time after expenditure of significant effort and
4 resources.

5 325. Cisco trade secrets are not publicly available, and are kept within the knowledge and
6 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
7 bound by contractual obligations of confidentiality.

8 326. Cisco has taken reasonable measures to keep its trade secret information secret.

9 327. Cisco communicates the importance of maintaining confidentiality to its employees in
10 various means and forms, including but not limited to the Proprietary Information and Inventions
11 Agreements and termination letters.

12 328. Cisco implements security measures such as electronic access points to restrict access
13 to Cisco's confidential and proprietary information.

14 329. Cisco trade secrets derive independent economic value, actual or potential, from not
15 being generally known to, and/or not being readily ascertainable through proper means by, the public
16 or other persons who can obtain economic value from the disclosure or use of the information.

17 330. Cisco's trade secrets at issue in this case are related to products that are placed in or are
18 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
19 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
20 1836.

21 331. Defendant Poly's misappropriation of Cisco's trade secret information was willful and
22 malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and
23 its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

24 332. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

25 333. On information and belief, if Defendant Poly's conduct is not remedied and/or
26 enjoined, Defendant will continue to misappropriate, disclose, and use for its own benefit and to
27 Cisco's detriment Cisco's trade secret information.

28

334. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Poly's continued misappropriation of Cisco's trade secret information.

COUNT XI

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Poly

335. Paragraphs 1 through 334 are incorporated by reference as if fully stated herein.

336. Poly's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

337. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

338. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

339. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

340. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for its own benefit and to Cisco's detriment Cisco's trade secret information.

341. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code § 3426.2.

COUNT XII

Intentional Interference with a Contractual Relationship by Poly

342. Paragraphs 1 through 341 are incorporated by reference as if fully stated herein

Prayer For Relief

G. Such other and further relief as this Court deems just and proper.

Plaintiff Cisco hereby demands a trial by jury on all issues so triable.

Dated: December 17, 2019

By: /s/ John M. Desmarais

John M. Desmarais (SBN 320875)
DESMARAIS LLP
101 California Street
San Francisco, CA 94111
(415) 573-1900

Tamir Packin (SBN 317249)
Carson Olsheski (*pro hac vice* pending)
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
212-351-3400

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that, on this day, I caused to be served the foregoing FIRST AMENDED COMPLAINT FOR TRADE SECRET MISAPPROPRIATION on counsel for defendants Wilson Chung and Jedd Williams in this action via e-mail transmission to each of the electronic addresses listed below. I further certify that counsel for defendant James He will be served via CM/ECF upon filing.

Counsel for Defendant Wilson Chung:

Daniel Muller
Ventura Hersey & Muller LLP
1506 Hamilton Avenue
San Jose, CA 95125
Tel: 408-512-3022
Email: dmuller@venturahersey.com

Counsel for Defendant Jedd Williams

Alison Plessman
Hueston Hennigan
523 West 6th Street, Suite 400
Los Angeles, CA 90014
Tel: 213-788-4340
Email: aplessman@hueston.com

Dated: December 17, 2019

/s/ John M. Desmarais
John M. Desmarais